Snare System Toronto

Symtrex offers several distinctly different IT security services and products for our clients. Our expertise in the aspect of network security as it pertains to evolving regulations, standards and security compliance is in high demand. In bridging this information need, you will find throughout our web site that we have endeavored to provide all the building blocks necessary to educate our clients and their personnel on the security aspects of their respective security standards as they pertain to their infrastructure. The peace of mind we provide to our clients is immeasurable.

From our beginnings over 25 years ago, we make sure everything we do honors this commitment to the highest security standards available to guarantee that peace of mind, with well recognized and respected brands in each of our principal markets, as well as investigating and researching new product offerings to address the latest threats and advances to counter these threats . We work with our clients as we do with our partners. We help build internal capabilities, get to the real issues and reach practical recommendations.

The security environment is in constant flux with threats continuously adapting and finding new ways to breach the latest security measures. In order to deal with this constant threat, security systems must be updated on a regular basis. Symtrex stays at the head of the field keeping abreast of the latest network security software, IT security compliance systems and compliance reporting systems.

Snare Product Suite

Centralized Log Management and Analysis is essential to assuring the integrity of critical logs, achieving compliance with the growing list of regulations, and internal security requirements.

The process of transmitting log files across public or even private networks can work against these objectives. The ability to perform these tasks in the past have been complicated, costly and time consuming, until now.

The SNARE Product Suite is a Security Information Management tool which is comprised of two components – SNARE agents and the SNARE Server. The system, which is developed by Intersect Alliance, is one of the most comprehensive tools, providing real time data collection,

monitoring console, data filtering and event aggregation at the source through the use of the SNARE agents.

The Snare Product Suite Overview

The Snare System provides clear, concise, accurate reporting of the information that is pertinent to your organizations security and audit requirements. Download the Snare System Datasheet

The Snare Server provides a dashboard to view of all pertinent audit events from a heterogeneous network. All incoming events (from Snare Agents and from system log enabled devices) are received into a Snare Server enabling them to be analyzed, recorded and reported based on the corporate audit requirements. The Snare Server has a large library of security objective reports, in addition to the ability to create adhoc reports or adjust the templated security objectives, providing flexibility to an organizations reporting structure. These comprehensive reports can then be automatically emailed to the security individual responsible for those systems and audit requirements on a daily, weekly or monthly basis. The reports can also be viewed from the web interface interactively.

The Snare Agents have been developed for a number of applications and operating systems such as Windows, Solaris, AIX, Irix, Linux, ISA, IIS, etc. The Agents are installed and configured on systems that are to be monitored for specific audit activity. They forward only those events that match the configured audit criteria to the Snare Server. The Open Source Agents are licensed under GPL and can be downloaded from sourceforge.

The Snare Enterprise Agents have been developed for use with the Snare Server or other SIEM product and provide added functionality. The Enterprise agents have been developed for Windows, Solaris, Linux, AIX, Irix plus two Epilog Agents for Windows and Unix which enable collection of the application log files for such items as ISA, IIS, Exchange, Squid, and Apache. In addition there is an MS SQL Agent. As well they have just released three new agents – Snare Agent for MAC OSX, and two browser agents – Firefox and Chrome.

Snare Server

The Snare Server provides a dashboard view of all pertinent information from a corporation's heterogeneous network. It collects log files from a variety of operating systems, applications and appliances, as well as the Snare Agents. These include, but are not limited to: Windows , Solaris, AIX, Irix, Linux, Tru64, ACF2, CISCO Routers, CISCO PIX Firewall, CyberGuard Firewall, Checkpoint Firewall1, Netgear Firewall, IPTables Firewall, Microsoft ISA Server, Microsoft IIS Server, Lotus Notes, Microsoft Proxy Server, Apache, Squid, Snort Network Intrusion Detection Sensors, IBM SOCKS Server, and Generic Syslog Data of any variety. As well as text based log files and MS SQL.

The benefits of the Snare system are:

- Ability to collect any arbitrary log event
- Ability to collect large numbers of events – over 30,000 events per minute on a low-end Intel-based workstation
- Automatic archiving of events to compressed text, allowing optimization of database functionality
- Unique methods for administrators to 'fine-tune' reporting criteria
- Ability to create dynamic reports allowing reporting against any collection profile.
- Ability to use and filter event log collection methods with or without Snare Agents
- Annual maintenance includes access to all future Snare System upgrades and new versions
- Development of the Snare System is guided by its users – they use it daily and know what they need – and we can develop it for you and give you the skills to support all enhancements
- Unique and powerful forensic analysis tools used worldwide
- The only system that provides support to 'Snare Agents' anywhere in the world
- Pricing options that are more than competitive against the competition
- Experienced support team who have been working with 'Event Log Management' concepts longer than anyone else and whose tools are more widely used than any other Event Log Management tool worldwide

The Snare System's return on investment includes:

- Lower cost of labor through automation of reporting and critical event identification
- Less traffic on IT networks and systems – less overhead on your operating systems and less strain on your networks, reducing cost on maintenance, monitoring and support
- Capture event log data from any system using our own resources – not 3rd party – thus reducing cost
- Automation of audit and compliance functionality, using less resources
- Effective business continuity by providing a means to manage and lessen risk across the enterprise
- Instant methods of monitoring user activity and identifying suspect trends and events
- Effective utilization of your enterprise by allowing users to manage and monitor specific events for systems instead of investigating on a system to system basis

For more information please visit our website

http://www.symtrex.com/security-solutions/snare-system/snare-server